

WARD, KEENAN & BARRETT, P.C.

Gerald Barrett, SBN: 005855
3838 N. Central Avenue, Suite 1720
Phoenix, Arizona 85012
Tel: (602) 279-1717
Fax: (602) 279-8908
E-Mail: gbarrett@wardkeenabarrett.com

BURSOR & FISHER, P.A.

Yitzchak Kopel*
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: ykopel@bursor.com

**pro hac vice forthcoming*

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Nancy Encinas, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

Office Depot, LLC,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiff Nancy Encinas, individually and on behalf of all others similarly
2 situated, as set forth herein, alleges as follows:

3 **NATURE OF THE ACTION**

4 1. This is a class action on behalf of persons in the State of Arizona that
5 opened emails sent to them by Defendant Office Depot, LLC (“Defendant” or
6 “Office Depot”) due to Defendant’s violations of Arizona’s Telephone, Utility and
7 Communication Service Records Act, A.R.S. § 44-1376 *et seq.*

8 2. Defendant is one of the nation’s leading providers of office and
9 business supplies, services, products and technology solutions. Defendant has over
10 900 retail store locations across the United States, including 23 stores in Arizona.
11 To entice residents to visit their stores and to maximize sales, Defendant solicits
12 customers to sign up for its email list.

13 3. Plaintiff and Class members are subscribers to Defendant’s email list.

14 4. Defendant embeds hidden spy pixel trackers within its emails. These
15 trackers capture and log sensitive information including the time and place
16 subscribers open and read their messages, how long it takes the subscriber to read
17 the email, subscribers’ location, subscribers’ email client type, subscribers’ IP
18 address, subscribers’ device information and whether and to whom the email was
19 forwarded to. Defendant never received subscribers’ consent to collect this private
20 information.

21 5. Defendant’s invasive surveillance of Plaintiff’s sensitive reading habits
22 and clandestine collection of her confidential email records invaded her privacy and
23 intruded upon her seclusion.

24 6. By failing to receive consent from Plaintiff and Class members,
25 Defendant is violating Arizona’s Telephone, Utility and Communication Service
26 Records Act, a statute that prohibits procuring or attempting to procure the
27 communication service records of email recipients without their authorization.
28

THE PARTIES

7. Plaintiff is a resident of Arizona, residing in Casa Grande, Arizona. Within the past two years, Plaintiff has received promotional emails from Defendant.

8. From approximately January 2024 to June 2024, Plaintiff frequently opened emails from Defendant to review promotional materials. Plaintiff most recently opened one of Defendant's emails in June 2024.

9. Each time Plaintiff opened an email from Defendant, Defendant procured her sensitive email information including the time and place she opened and read the messages, how long she read the email, her location, her email client type, her IP address, her device information and whether and to whom the email was forwarded to.

10. Defendant never received consent from Plaintiff to procure her private email records.

11. Defendant Office Depot, LLC is a Delaware corporation with its principal place of business in Boca Raton, Florida. Defendant owns and operates 23 Office Depot stores in the state of Arizona.

JURISDICTION AND VENUE

12. The Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A), as amended by the Class Action Fairness Act of 2005 ("CAFA"), because this case is a class action where the aggregate claims of all members of the proposed class are in excess of \$5,000,000.00, exclusive of interest and costs, and there are over 100 members of the putative class, and Plaintiffs, as well as most members of the proposed class, are citizens of different states than Defendant.

13. The Court has personal jurisdiction over Defendant because Defendant has purposefully availed itself of the laws and benefits of doing business in this State, and Plaintiff's claims arise out of Defendant's forum-related activities. Furthermore, a substantial portion of the events giving rise to Plaintiff's claims

1 occurred in this District.

2 14. Venue is proper in this District because a substantial part of the events,
3 omissions, and acts giving rise to the claims herein occurred in this District.

4 **FACTS SUPPORTING PLAINTIFF'S CLAIM**

5 **A. The HP Spying Scandal and A.R.S. § 44-1376**

6 15. In 2001, Hewlett-Packard “embark[ed] on one of the largest and most
7 difficult mergers in American business history.”¹ Spearheaded by then-CEO Carly
8 Fiorina, HP sought to acquire a rival company, Compaq, Inc., in a deal valued at
9 \$25 billion.²

10 16. “Widely considered one of the worst tech mergers in history,”³ the
11 economic fallout from the acquisition began immediately.⁴ By 2004, “Hewlett-
12 Packard’s stock had dropped below seventeen dollars, from a high of more than
13 sixty dollars, in 2000.”⁵ Industry insiders took note, with a “consensus” believing
14 that “the new HP, the tech industry’s most sprawling conglomerate, ha[d] lost its
15 focus and [was] being squeezed between two formidable rivals with much clearer
16 business models, Dell and IBM.”⁶

17 ¹ Michael Malone, *The H-P-Compaq Mess Isn’t All Carly’s Doing*, WALL. ST. J.
18 (May 21, 2002), <https://www.wsj.com/articles/SB1021933260918245440>.

19 ² Andrew Ross Sorkin, *Hewlett-Packard in Deal to Buy Compaq for \$25 Billion in*
20 *Stock*, N.Y. TIMES (Sept. 4, 2001),
21 [https://www.nytimes.com/2001/09/04/business/hewlett-packard-in-deal-to-buy-](https://www.nytimes.com/2001/09/04/business/hewlett-packard-in-deal-to-buy-compaq-for-25-billion-in-stock.html)
22 [compaq-for-25-billion-in-stock.html](https://www.nytimes.com/2001/09/04/business/hewlett-packard-in-deal-to-buy-compaq-for-25-billion-in-stock.html).

23 ³ PCMag Staff, *The Biggest Tech Mergers and Acquisitions of All Time*, PCMAG
24 (Apr. 12, 2021), [https://www.pcmag.com/news/the-biggest-tech-mergers-and-](https://www.pcmag.com/news/the-biggest-tech-mergers-and-acquisitions-of-all-time)
25 [acquisitions-of-all-time](https://www.pcmag.com/news/the-biggest-tech-mergers-and-acquisitions-of-all-time).

26 ⁴ Mike Musgrove, *HP Posts \$2 Billion Loss in First Full Quarter with Compaq*,
27 WASH. POST (Aug. 28, 2002),
28 [https://www.washingtonpost.com/archive/business/2002/08/28/hp-posts-2-billion-](https://www.washingtonpost.com/archive/business/2002/08/28/hp-posts-2-billion-loss-in-first-full-quarter-with-compaq/2486859a-b55c-4247-9f0a-cb1d839b68d8/)
loss-in-first-full-quarter-with-compaq/2486859a-b55c-4247-9f0a-cb1d839b68d8/.

⁵ James Stewart, *The Kona Files*, THE NEW YORKER (Feb. 11, 2007),
<https://www.newyorker.com/magazine/2007/02/19/the-kona-files>.

⁶ The Economist Staff, *Losing the HP way*, THE ECONOMIST (Aug. 19, 2004),
<https://www.economist.com/business/2004/08/19/losing-the-hp-way>.

1 17. In January 2005, a few days before HP's annual retreat, two board
2 members, Patricia Dunn and George Keyworth, met with Fiorina to discuss their
3 concerns about the company's direction.⁷ Fiorina sought to placate Dunn and
4 Keyworth, "agree[ing] to tear up her agenda for the board's strategy retreat ... and
5 focus instead on the directors' concerns."⁸ But shortly after the retreat, "a reporter
6 for the *Wall Street Journal*, Pui-Wing Tam, called to confirm details that Tam had
7 learned about the retreat, including assertions that Fiorina had lost the confidence of
8 the board and that operating responsibilities would soon be shifted away from her."⁹
9 "Clearly, someone at the retreat, which was attended only by board members and
10 top executives, had leaked proprietary information."¹⁰

11 18. Fiorina responded with fury. After "call[ing] the board members
12 together on the phone," Fiorina "dressed them down for giving details of the
13 meeting."¹¹ But that response only further inflamed tensions between Fiorina and
14 the board, and less than two weeks after the retreat, the board met again, this time
15 without Fiorina, and voted to dismiss her.¹²

16 19. Despite Fiorina's departure, board members remained perturbed by the
17 disclosures to the press, and so when elevating Patricia Dunn to nonexecutive
18 chairwoman and tasking her with choosing Fiorina's successor, the board also
19 provided Dunn with another mandate: "stop the board leaks."¹³

20
21 ⁷ James Stewart, *The Kona Files*, THE NEW YORKER (Feb. 11, 2007),
<https://www.newyorker.com/magazine/2007/02/19/the-kona-files>.

22 ⁸ Alan Murray, H-P Board Clash Over Leaks Triggers Angry Resignation, WALL
23 ST. J. (Sept. 6, 2006), <https://www.wsj.com/articles/SB115749453036454340>.

24 ⁹ James Stewart, *The Kona Files*, THE NEW YORKER (Feb. 11, 2007),
<https://www.newyorker.com/magazine/2007/02/19/the-kona-files>.

25 ¹⁰ *Id.*

26 ¹¹ Alan Murray, H-P Board Clash Over Leaks Triggers Angry Resignation, WALL
ST. J. (Sept. 6, 2006), <https://www.wsj.com/articles/SB115749453036454340>.

27 ¹² *Id.*

28 ¹³ James Stewart, *The Kona Files*, THE NEW YORKER (Feb. 11, 2007),
<https://www.newyorker.com/magazine/2007/02/19/the-kona-files>.

20. Dunn promptly initiated an investigation, code-naming it “Project Kona.”¹⁴ But before Project Kona could get off the ground, another more damaging leak came to light.¹⁵ In the months after Fiorina’s removal, Dunn selected Mike Hurd, a CEO at a competitor company, to serve as HP’s new CEO.¹⁶ However, before the board could make an announcement, a reporter from *Business Week* reached out, asking for comment on Hurd’s selection.¹⁷ Because Hurd had not yet left the other company, revealing his candidacy before he resigned could potentially derail the process.¹⁸ Although Hurd would go on to become HP’s CEO without issue, the new disclosure added urgency to determining who was behind the leaks.¹⁹ For Dunn, Project Kona was the way to find out.²⁰

21. To staff Project Kona, Dunn turned to a security manager at HP, Kevin Huska, who, in turn, “referred Dunn to an outside investigator named Ronald R. DeLia, whose firm, Security Outsourcing Solutions, based in Boston, had been under contract to Hewlett-Packard for some ten years.”²¹ Throughout the summer of 2005, Dunn received regular updates from DeLia, including one call where he “revealed that his investigators had obtained private phone records of reporters.”²² DeLia received these records through “pretexting,” which, in his own words, “involved investigators requesting information from [telephone] operators orally, over the phone, pretending to be someone else if necessary.”²³ Notwithstanding this invasion of privacy, Project Kona failed to pinpoint a leaker, and as the year winded

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

²³ *Id.*

1 down, so too did the investigation.²⁴

2 22. Then, in January 2006, a reporter from CNET named Dawn
3 Kawamoto published an “inside account of the company’s retreat, held two weeks
4 earlier.”²⁵ The substance of the article was innocuous, but at HP, “the story was
5 met with alarm.”²⁶ In response to the leak, “[a] new investigation was immediately
6 launched, which Dunn called Kona II.”²⁷ HP’s general counsel, Ann Baskins,
7 “asked an employment lawyer at the company, Kevin Hunsaker, to head the
8 renewed investigation.”²⁸ “With Hunsaker in day-to-day charge, the investigators
9 undertook their mission with extraordinary zeal,” pretexting phone companies to
10 obtain records for reporters, directors, and employees.²⁹

11 23. In addition to pretexting, the investigators also took a new approach.³⁰
12 Posing as a disgruntled employee, they emailed Kawamoto with the promise of
13 revealing damaging information about the company.³¹ Unbeknownst to Kawamoto,
14 the investigators utilized “ReadNotify,” a tracker that, once embedded into an
15 email, allowed them to “track the path [the] message takes, including whether [the]
16 recipient opens the message.”³² “[A] technique also employed by some e-mail
17 marketers,”³³ the investigators hoped that Kawamoto would “forward the e-mail to
18 her source,” thereby revealing who had leaked the confidential information.³⁴

19 ²⁴ *Id.*

20 ²⁵ *Id.*

21 ²⁶ *Id.*

22 ²⁷ *Id.*

23 ²⁸ *Id.*

24 ²⁹ *Id.*

25 ³⁰ *Id.*

26 ³¹ *Id.*

27 ³² Robert McMillan, *HP’s e-mail tracer in widespread use*, COMPUTERWORLD (Oct.
28 10, 2006), <https://www.computerworld.com/article/2820287/hp-s-e-mail-tracer-in-widespread-use.html>

29 ³³ *Id.*

30 ³⁴ Joris Evers, *How HP bugged e-mail*, CNET (Sept. 29, 2006),
<https://www.cnet.com/news/privacy/how-hp-bugged-e-mail/>.

24. ReadNotify failed to yield results, with Kawamoto declining to forward the email.³⁵ But this time around, after combing through the phone records, investigators discovered that a board member, George Keyworth, had a short conversation with Kawamoto right before the article was published.³⁶ After the revelation, the board confronted Keyworth, who admitted to having lunch with the reporter and “say[ing] some nice things about Mike Hurd.”³⁷ The board responded by voting on a motion to request Keyworth’s resignation.³⁸ After the motion passed, a board member who dissented, Mark Perkins, quit in protest.³⁹ Keyworth, for his part, refused to step aside, “saying the shareholders had elected him, and he felt the punishment was out of proportion to the offense.”⁴⁰

25. Perkins did not go quietly.⁴¹ After resigning from the board, Perkins retained a lawyer, Viet Denh, who “contacted the S.E.C., the U.S. Attorney’s offices in Manhattan and San Francisco, the California Attorney General, the F.C.C., and the F.T.C.”⁴²

26. Once HP’s tactics were made public, the reaction was swift and overwhelming. In September 2006, Congress held a hearing on the scandal, asking Dunn and other witnesses to answer two questions: “Exactly what did they know about the use of pretexting,” and “[w]hat did they know about planting spyware on an email to a journalist.”⁴³ The witnesses verified that investigators employed both

³⁵ James Stewart, *The Kona Files*, THE NEW YORKER (Feb. 11, 2007), <https://www.newyorker.com/magazine/2007/02/19/the-kona-files>.

³⁶ *Id.*

³⁷ *Id.*

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.*

⁴³ Hewlett-Packard's Pretexting Scandal: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce, 109th Cong. 45 (2006), <https://www.govinfo.gov/content/pkg/CHRG->

1 methods to gather evidence, but they maintained that their conduct was lawful.⁴⁴
 2 Throughout the hearing, members of Congress called for a law that would prohibit
 3 these practices, with one member remarking that “[t]he growing market for
 4 personal information is enormous, and many of us have seen this, and that is why
 5 we need to pass legislation to stop this.”⁴⁵ When another member asked Dunn
 6 whether it “strike[s] you as a permissible tactic to use, attaching a tracking device
 7 onto an e-mail,” Dunn replied, “[i]t is kind of surprising that it is legal, isn’t it?”⁴⁶
 8 Still another member lamented that email trackers were “equivalent to going
 9 through the mail in my mailbox.”⁴⁷

10 27. Six days after the hearing, the California Attorney General indicted
 11 Dunn, Hunsaker, DeLia, and two private investigators involved in both iterations of
 12 Project Kona.⁴⁸ A few months after that, Congress passed the Telephone Records
 13 and Privacy Protection Act of 2006, a law that criminalizes “knowingly and
 14 intentionally obtain[ing], or attempt[ing] to obtain, confidential phone records
 15 information of a covered entity, by making false or fraudulent statements or
 16 representations to an employee of a covered entity.” 18 U.S.C. § 1039(a)(1). That
 17 law, as the text suggests, only prohibits pretexting, not the use of email trackers.

18 28. After Congress enacted the Telephone Records and Privacy Protection
 19 Act of 2006, the Arizona legislature went a step further, passing a law that
 20 addressed *both* methods used by HP’s investigators. Like the federal law, this new
 21 Arizona law prohibits any person from procuring or conspiring with another to
 22 procure “a telephone record” of residents without consent. But, in addition, the
 23

24 109hhrg31472/html/CHRG-109hhrg31472.htm.

25 ⁴⁴ *Id.*

26 ⁴⁵ *Id.*

27 ⁴⁶ *Id.*

28 ⁴⁷ *Id.*

⁴⁸ James Stewart, *The Kona Files*, THE NEW YORKER (Feb. 11, 2007),
<https://www.newyorker.com/magazine/2007/02/19/the-kona-files>.

new law also prohibits procurement of any “communication service record” (including email records) of “any resident of this state without the authorization of the customer to whom the record pertains, or by fraudulent, deceptive, or false means.” Ariz. Rev. Stat. Ann. § 44-1376.01. And while Congress declined to include a private right of action in the federal law, the Arizona legislature allowed residents to pursue civil remedies. Ariz. Rev. Stat. Ann. § 44-1376.04(2).

B. Email Pixels

29. Despite Arizona law prohibiting the practice, companies still embed trackers within emails without first obtaining consumers’ consent. Indeed, “[a] 2018 Princeton study on email tracking tested over 12,000 emails from 900 senders offering mailing list subscriptions and found that 70% contained trackers.”⁴⁹

30. These trackers, known as “spy pixels,” enable companies to learn information about the email transmission, including when and where the email was opened. Pixels are used to log when the recipient accesses the email and can record the number of times an email is opened, the IP address linked to a user’s location, and device usage.⁵⁰

31. Spy pixels can also monitor how long the recipient spends reading the email, whether the email was forwarded, and whether the recipient prints the email.⁵¹

32. The use of spy pixels is a “grotesque invasion of privacy” according to

⁴⁹ Mikael Berner, *The Business of Email Tracking: What To Know About Spy Pixels In Your Inbox*, FORBES (Jun 9, 2022), <https://www.forbes.com/sites/forbestechcouncil/2022/06/09/the-business-of-email-tracking-what-to-know-about-spy-pixels-in-your-inbox/?sh=2084ee793fec>.

⁵⁰ Charlie Osborne, *Tracker pixels in emails are now an ‘endemic’ privacy concern*, ZDNET (Feb. 17, 2021), <https://www.zdnet.com/article/spy-pixels-in-emails-to-track-recipient-activity-are-now-an-endemic-privacy-concern/>.

⁵¹ https://knowledge.validity.com/s/articles/Everest-Engagement-Playbook-Beginner?language=en_US

1 industry advocates.⁵²

2 33. To activate a spy pixel, recipients only need to open the email. The
3 recipient does not need to directly engage with the pixel—when an email is opened
4 the tracking pixel is automatically downloaded.⁵³

5 34. A spy pixel is typically a 1x1 (one pixel high by one pixel long) image.
6 “The spy pixel is so small it is basically impossible to see with the naked eye.”⁵⁴

7 35. The spy pixel used by marketers today operates the same way as the
8 spy pixels in the HP pretexting scandal—email activity including who accessed an
9 email, as well as when and where an email was accessed, is procured through the
10 same technology, an invisible pixel embedded in the email code that allows the
11 sender to log and track that information.

12 **C. Defendant’s Spy Pixel Tracking**

13 36. Defendant uses spy pixels to track when customers open their emails,
14 as pictured in the example below. That tracker records the email address, the
15 subject of the email, when the email is opened and read, the recipient’s location,
16 how long the recipient spends reading an email, whether it is forwarded, whether it
17 is printed, and what kind of email server the recipient uses, among other sensitive
18
19
20
21
22
23

24 ⁵² *Charlie Osborne, Tracker pixels in emails are now an ‘endemic’ privacy*
25 *concern, ZDNET (Feb. 17, 2021), [https://www.zdnet.com/article/spy-pixels-in-](https://www.zdnet.com/article/spy-pixels-in-emails-to-track-recipient-activity-are-now-an-endemic-privacy-concern/)*
26 *emails-to-track-recipient-activity-are-now-an-endemic-privacy-concern/.*

27 ⁵³ *Id.*

28 ⁵⁴ *Becky Willeke, Spy pixels are hiding in your emails; so what can you do about*
it?, Fox 2 Now (Mar. 15, 2021), [https://fox2now.com/news/tech-talk/spy-pixels-](https://fox2now.com/news/tech-talk/spy-pixels-are-hiding-in-your-emails-so-what-can-you-do-about-it/)
are-hiding-in-your-emails-so-what-can-you-do-about-it/.

information.

```
<img src=3D"https://data.em.officedepot.com/ee/v1/open?params=
pid=
uid=
onfigId= " width=3D"1" height=3D"1">
```

37. The spy pixel uses a custom URL that is specific for each recipient and each email.

```
<img alt=3D"" aria-hidden=3D"true" height=3D"1" src=3D"http://mi.of
ficedepot.com/p/up/
&mi_ecmp=
&mi_ign= " width=3D"
1">
```

38. Defendant also hides trackers within images embedded within emails through the use of spy tracking pixels from Movable Ink.

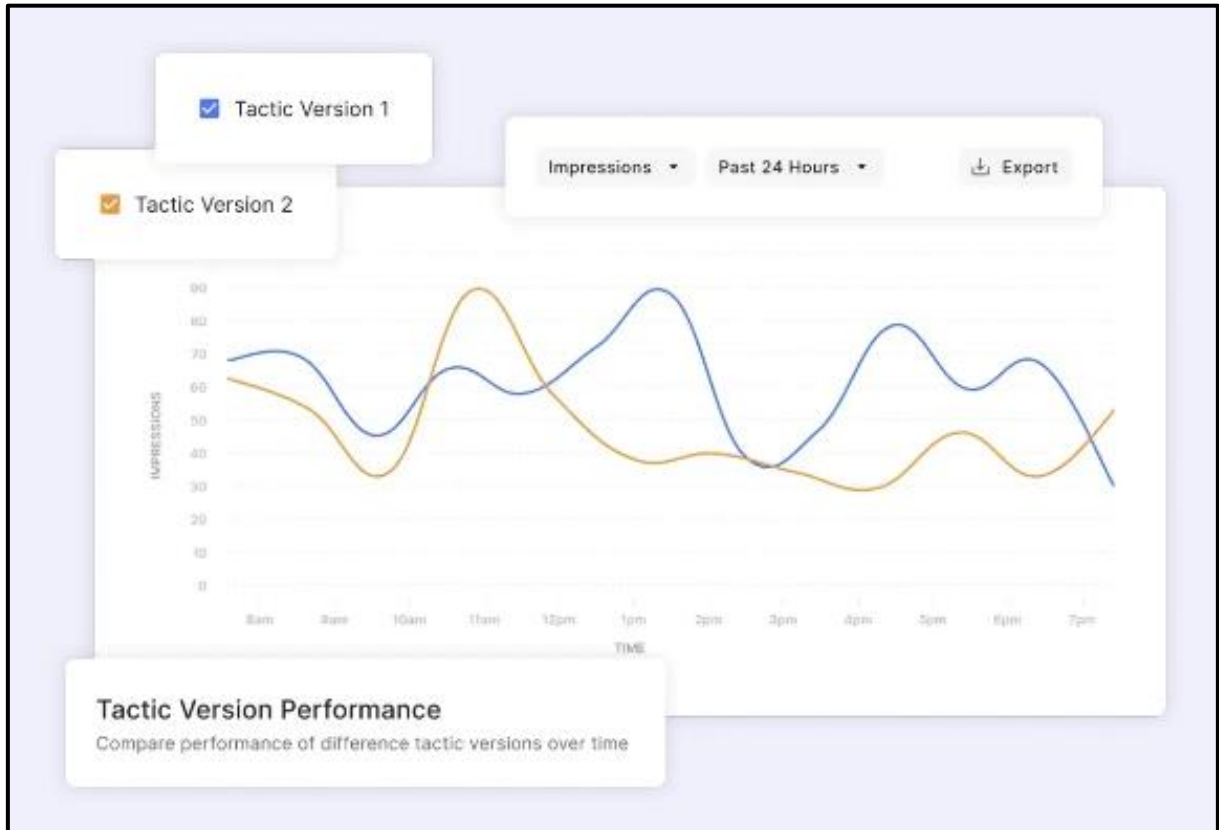
39. The “mi_u” parameter identifies the recipient’s Movable Ink customer ID⁵⁵ so that Movable Ink can provide Defendant analytics about how many “impressions”—email opens—the email received.⁵⁶

40. Defendant uses Movable Ink to “build custom data visualizations” to analyze email recipients “metrics” such as “clicks, conversions, revenue, and impressions” and sort them by “by common variables such as campaign,

⁵⁵ https://docs.oracle.com/en/cloud/saas/marketing/infinity-user/Help/integrate/movableink/movableink_faq.htm

⁵⁶ <https://movableink.com/studio>

deployment, block, device, date, and more.”⁵⁷



41. Plaintiff was unaware that tracking pixels were embedded in the emails as Defendant does not inform users it embeds tracking pixels in its marketing emails. Defendant never received consent from Plaintiff and Class Members to use these spy pixels.

CLASS ACTION ALLEGATIONS

42. Plaintiff seeks to represent a class (the “Class”) defined as: All persons within Arizona who have opened a marketing email containing a tracking pixel from Defendant.

43. Excluded from the Class are Defendant, its subsidiaries, affiliates, officers, directors, assigns and successors, and any entity in which it has a controlling interest, and the Judge to whom this case is assigned and any member of his or her immediate family.

⁵⁷ <https://movableink.com/studio>

1 44. Members of the Class are so numerous that their individual joinder
2 herein is impracticable. On information and belief, members of the Class number
3 in the hundreds of thousands. The precise number of Class members and their
4 identities are unknown to Plaintiff at this time but will be determined through
5 discovery. Class members may be notified of the pendency of this action by mail
6 and/or publication through the distribution records of Defendant and third-party
7 retailers and vendors.

8 45. Common questions of law and fact exist as to all Class members and
9 predominate over questions affecting only individual Class members. Common
10 legal and factual questions include, but are not limited to:

- 11 a) whether Defendant “[k]nowingly procure[d], attempt[ed] to procure,
12 solicit[ed] or conspire[d] with another to procure a ... communication
13 service record of any resident of this state without the authorization of
14 the customer to whom the record pertains or by fraudulent, deceptive or
false means” in violation of A.R.S. § 44-1376 *et seq.*;
- 15 b) whether Plaintiff’s and the Class’s “communication service records”
16 were procured, sold or received in violation of A.R.S. § 44-1376, *et seq.*
- 17 c) whether Defendant’s conduct violates A.R.S. § 44-1376, *et seq.* or any
18 other applicable laws; and
- 19 d) whether, as a result of Defendant’s misconduct as alleged herein,
20 Plaintiff and Class members are entitled to restitution, injunctive, and/or
21 monetary relief and, if so, the amount and nature of such relief.

22 46. Plaintiff’s claims are typical of the claims of Class members because
23 Plaintiff, like all Class members, had her communication service records procured,
24 sold, or received by Defendant.

25 47. Plaintiff is an adequate representative of the Class because her
26 interests do not conflict with the interests of the Class members she seeks to
27 represent, she has retained counsel competent and experienced in prosecuting class
28 actions, and she intends to prosecute this action vigorously. The interests of Class

1 members will be fairly and adequately protected by Plaintiff and her counsel.

2 48. The class mechanism is superior to other available means for the fair
3 and efficient adjudication of the claims of Plaintiff and Class members. Each
4 individual Class member may lack the resources to undergo the burden and expense
5 of individual prosecution of the complex and extensive litigation necessary to
6 establish Defendant's liability. Individualized litigation increases the delay and
7 expense to all parties and multiplies the burden on the judicial system presented by
8 the complex legal and factual issues of this case. Individualized litigation also
9 presents a potential for inconsistent or contradictory judgments. In contrast, the
10 class action device presents far fewer management difficulties and provides the
11 benefits of single adjudication, economy of scale, and comprehensive supervision
12 by a single court on the issue of Defendant's liability. Class treatment of the
13 liability issues will ensure that all claims and claimants are before this Court for
14 consistent adjudication of the liability issues.

15 **COUNT I**

16 **Violation of A.R.S. § 44-1376.01**

17 49. Plaintiff hereby incorporates by reference the allegations contained in
18 all preceding paragraphs of this complaint.

19 50. Plaintiff brings this claim individually and on behalf of the members of
20 the proposed Class against Defendant.

21 51. Defendant embeds spy pixels in its marketing emails sent to Plaintiff
22 and Class members.

23 52. The spy pixels are designed to extract "communication service
24 records" related to the delivery of the email in which the spy pixel is embedded.
25 This includes, but is not limited to, time logs of email access, logs of associated
26 email addresses, logs of email client type, logs of email path data, logs of recipient
27 location, logs of IP address, logs of email forwarding data, and logs of device
28

1 information.

2 53. Defendant “procures” Plaintiff’s and Class members’ “communication
3 service records” because they “obtain by any means, including electronically”
4 Plaintiff and Class member’s “communication service records” as defined in A.R.S.
5 § 44-1376.

6 54. In contravention of A.R.S. § 44-1376.01, Defendant knowingly
7 procures “subscriber information, including name, billing or installation address,
8 length of service, payment method, telephone number, electronic account
9 identification and associated screen names, toll bills or access logs, records of the
10 path of an electronic communication between the point of origin and the point of
11 delivery and the nature of the communication service provided, such as ...
12 electronic mail ...,” which constitute “communication service records” under
13 A.R.S. § 44-1376, from Plaintiff and Class members.

14 55. Plaintiff and Class members were never informed by Defendant, and
15 thus never knew, that Defendant would be procuring sensitive information
16 including, but not limited to, time logs of email access, associated email addresses,
17 email client type, email path data, IP addresses, and device information.

18 56. Plaintiff and Class members never gave lawful consent to Defendant to
19 procure the communication service records.

20 57. Each time Defendant sent an email containing a spy pixel, Defendant
21 procured a communication service record, thus committing a separate violation of
22 A.R.S. § 44-1376.01.

23 58. Defendant invaded Plaintiff’s and Class members’ right to privacy by
24 its invasive surveillance of Plaintiff’s and Class members’ sensitive reading habits,
25 including when they opened and read an email. This clandestine collection of their
26 confidential email records also intruded upon their seclusion.

27 59. Accordingly, Plaintiff, individually and on behalf of the proposed
28 Class, prays for the relief set forth by the statute, including actual damages, profits

made by Defendant as a result of the violation, \$1,000 for each violation, reasonable attorneys' fees and other litigation costs reasonably incurred, and such other equitable relief as the court determines to be appropriate.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

- a. For an order certifying the Class under Fed. R. Civ. P 23 and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class members;
- b. For an order declaring that Defendant's conduct, as set out above, violates A.R.S. § 44-1376.01;
- c. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- d. For actual damages or damages of \$1,000.00 for each of Defendant's violations, whichever is more, pursuant to A.R.S. § 44-1376.04;
- e. For damages equal to the sum of any profits Defendant made for each of Defendant's violations, pursuant to A.R.S. § 44-1376.04;
- f. For injunctive and other equitable relief as is necessary to protect the interests of the Class, including, inter alia, an order requiring Defendant to comply with A.R.S. § 44-1376, *et seq.*
- g. For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit;
- h. For pre- and post-judgment interest on all amounts awarded, to the extent allowable; and
- i. For such other and further relief as the Court may deem proper.

JURY DEMAND

Plaintiff demands a trial by jury on all causes of action and issues so triable.

Dated: June 17, 2024

Respectfully submitted,

WARD, KEENAN & BARRETT, P.C.

By: /s/ Gerald Barrett
Gerald Barrett

Gerald Barrett, SBN: 005855
3838 N. Central Avenue, Suite 1720
Phoenix, Arizona 85012
Tel: (602) 279-1717
Fax: (602) 279-8908
E-Mail: gbarrett@wardkeenanbarrett.com

BURSOR & FISHER, P.A.

Yitzchak Kopel*
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: ykopel@bursor.com

**pro hac vice forthcoming*

Attorneys for Plaintiff